IN THE CLAIMS:

The following listing of claims will replace all prior versions, and listings, of claims in the application.

1. (original) A processing unit connectable to a data communications network, the processing unit having a device reader for a portable storage device that includes storage operable to supply a network identity for the processing unit and an access controller, the access controller being operable to prevent unauthorised writing to the storage, the processing unit being operable, before reading the network identity from the portable storage device, to attempt a write to the storage of the portable storage device, and, on determining that the write has failed, to read the supplied network identity.

2. (previously presented) The processing unit of claim 1, wherein the processing unit is operable, on being powered up, to determine whether a said portable storage device is present in the device reader and, in the event that a said portable storage device is present in the device reader, to attempt a write to the storage of the portable storage device, the processing unit being further operable, on determining that the write has failed, to copy the supplied network identity from a data carrier to a second memory location and to use the supplied network identity.

3. (previously presented) The processing unit of claim 1, wherein access control logic of the portable storage device implements key-to-key encryption, the processing unit being operable to modify the content of the storage of the portable storage device by supplying a key to the access controller, and, in response to receipt of a return key from the access controller, to send an encrypted command to modify the content of the storage of the portable storage device.

4.   (original) The processing unit of claim 1, wherein the portable storage device is a smart card, the access controller is a microcontroller or a microprocessor, and the device reader is a smart card reader.

5.   (original) The processing unit of claim 1, wherein the network identity comprises a MAC address.

6.   (original) The processing unit of claim 1, comprising a service processor, the service processor being programmed to control reading of the portable storage device.

7.   (original) The processing unit of claim 6, wherein the service processor is a microcontroller.

8.   (original) The processing unit of claim 1, wherein the processing unit is a server computer.

9.   (original) The processing unit of claim 1, wherein the processing unit is a rack mountable computer server.

10.   (original) A control program for controlling the selection of a network identity for a processing unit connectable to a data communications network, the processing unit having a device reader for a portable storage device that includes storage operable to supply a network identity for the processing unit and an access controller, the access controller being operable to prevent unauthorised writing to the storage, the control program being operable, before reading the network identity from the portable storage device, to attempt a write to the storage of the portable storage device, and, only on determining that the write has failed, to read the supplied network identity.

11. (previously presented) The control program of claim 10, wherein the control program is operable, on the processing unit being powered up, to determine whether a said portable storage device is present in the device reader and, in the event that a said portable storage device is present in the device reader, to attempt a write to the storage of the portable storage device, the control program being further operable, on determining that the write has failed, to copy the supplied network identity from a data carrier to a second memory location and to use the supplied network identity.

12. (previously presented) The control program of claim 10, wherein access control logic of the portable storage device implements key-to-key encryption, the control program being operable to modify the content of the storage of the portable storage device by supplying a key to the access controller, and, in response to receipt of a return key from the access controller, to send an encrypted command to modify the content of the storage of the portable storage device.

13. (original) The control program of claim 10, wherein the portable storage device is a smart card, the access controller is a microcontroller and the device reader is a smart card reader.

14. (original) The control program of claim 10, wherein the network identity comprises a MAC address.

15. (original) The control program of claim 10 on a carrier medium.

16. (original) The control program of claim 10, wherein the processing unit comprises a service processor, the control program controlling operation of the service processor.

17. (original) The control program of claim 16, wherein the service processor is a microcontroller.

18.   (original) A microcontroller comprising a control program as recited in claim 10.

19.   (original) A server computer comprising a device reader for reading a portable storage, a processor, memory and a microcontroller as recited in claim 18, the microcontroller being operable as a service processor and connected to read the content of storage in a portable storage device mounted in the portable storage device.

20.   (currently amended) A method of controlling the selection of a network identity for a processing unit connectable to a data communications network, the processing unit having comprising a device reader for a portable storage device that includes storage operable to supply a network identity for the processing unit and an access controller, the access controller being operable to prevent unauthorised writing to the storage, the method comprising:
[-] attempting a write to the storage of the portable storage device; and
[-] only on determining that the write has failed, to read reading the supplied network identity from the portable storage device.

21.   (currently amended) The method of claim 20, further comprising:
[,] on powering up of the processing unit, determining whether a said portable storage device is present in the device reader; and
in the event that a said portable storage device is present in the device reader,
        [-] attempting a write to the storage of the portable storage device, and
        [-] only on determining that the write has failed, copying the supplied network identity from a data carrier to a second memory location and using the supplied network identity.

22.   (currently amended) The method of claim 20, wherein access control logic of the portable storage device implements key-to-key encryption, the method further comprising:

5

modifying the content of the storage of the portable storage device by supplying a key to the access controller[,]; and[,]

in response to receipt of a return key from the access controller, sending an encrypted command to modify the content of the storage of the portable storage device.

23.   (currently amended) The method of claim 20, wherein the portable storage device is a smart card, the access controller is a microcontroller, and the device reader is a smart card reader.

24.   (original) The method of claim 20, wherein the network identity comprises a MAC address.

25.   (original) A portable storage device that includes storage containing a network identity for a processing unit connectable to a data communications network, the portable storage device further including an access controller operable to prevent unauthorised writing to the storage, access controller being responsive to an unauthorised attempt to write to the storage to indicate that the write access has failed.

26.   (original) The portable storage device of claims 25, further operable to respond to a read access to supply the network identity.

27.   (original) The portable storage device of claim 25, wherein the access controller implements key-to-key encryption, the access controller including key storage holding a stored key, the access controller being operable to compare a supplied key from the processing unit to the stored key and, in response to the supplied key verifying against the stored key, returning to the processing unit a return key derived from the stored key.

28.   (original) The portable storage device of claim 27, wherein the access controller is subsequently operable to respond to an encrypted command from the processing unit to modify the content of the storage in the portable storage device.

29.   (original) The portable storage device of claim 25, wherein the access controller is a microcontroller.

30.   (original) The portable storage device of claim 25, wherein the portable storage device is a smart card.

31.   (original) The portable storage unit of 25, wherein the network identity comprises a MAC address.